DELTA RISK

CYBER SECURITY | BUSINESS RESILIENCY | RISK MANAGEMENT

CYBER EXERCISE

ACHIEVING VALUE THROUGH INNOVATIVE DESIGN BEST-PRACTICES

Presented to

6th Annual GFIRST National Conference

San Antonio, Texas

17 July 2010

Chris Fogle, CISSP

Delta Risk, LLC

DELTA RISK

CYBER SECURITY | BUSINESS RESILIENCY | RISK MANAGEMENT

- Cyber security & risk management group
- Public-private partnerships in Cyber and Homeland Security
- Principals with 50+ years experience in National Security-

  cyber warfare, tactics, and training

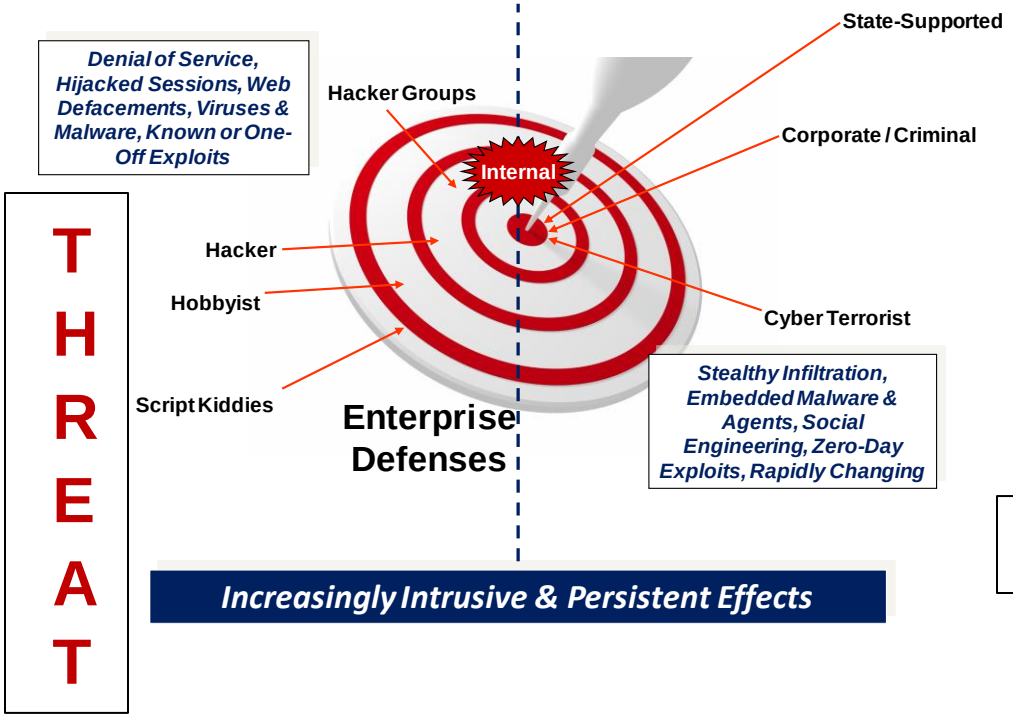
  - Planning and execution of DOD/national cyber defense exercises
  - BLACK DEMON, DARK SCREEN, Livewire, Cyber Storm, BULWARK DEFENDER

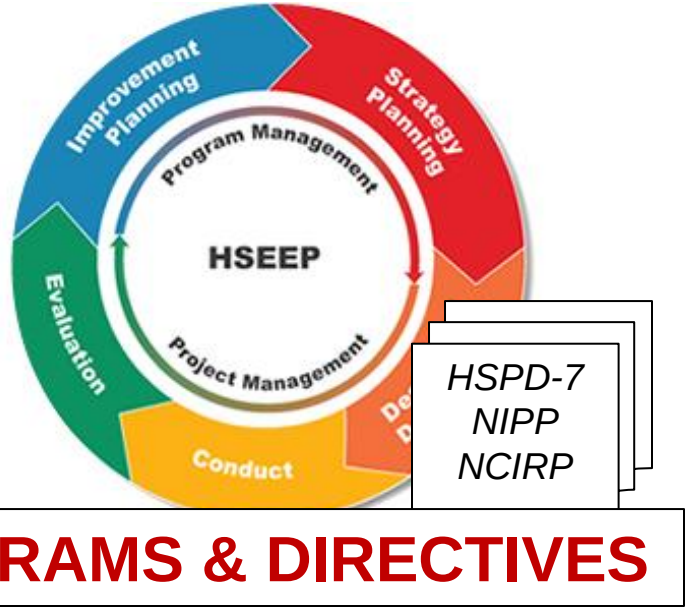
- Experience in large enterprise network security & defense, and business continuity
  - Focus on “demonstrated response” vs. “documented compliance”
  - Design and execute cyber defense training and assessment events against realistic threats

Overview

- Cyber exercises are increasingly important tools for training, assessing, and sharing information
- State of the Art not where it could be; need to “raise the bar”
- Better (more advanced, more value-added) cyber exercises are possible with a little creativity and some evolving technologies

Relevant landscape for cyber exercises…





… increasing attention

… recognized value

…what we mean by “Advanced Cyber Exercise”

CONTEXT

What is an "Exercise"…?

Evaluation

- *Standardization*
- *People & Positions*

Test

- *New procedures*
- *Technologies*

Assessment

- *Discover vulnerabilities*
- *Defenses (capacity & metrics)*

Drill

- *Training & Practice*

Exercise

More accurate than talking about it … when it's done right

More realistic training for your staff

Best test of combined people, processes, and technology

What is a "Cyber Exercise"…?

- Cyberspace
  - Interdependent domain … information infrastructures … Internet, telecommunications, computers, and embedded systems
- Cyber Attack
  - Attack … targeting enterprise's use of cyberspace … disrupting, disabling, destroying, or maliciously controlling … infrastructure, data, information, operations
- Cyber Incident
  - Actions through networks that result in … adverse affect on information system or information therein

Adapted from: Committee on National Security Systems (CNSS) Instruction 4009, National Information Assurance (IA) Glossary, 26 Apr 2010

Cyber Exercise … objectives focus on protecting, defending, and recovering cyber assets and operations from a cyber attack or cyber incident

HSEEP handles the science of exercises fairly well

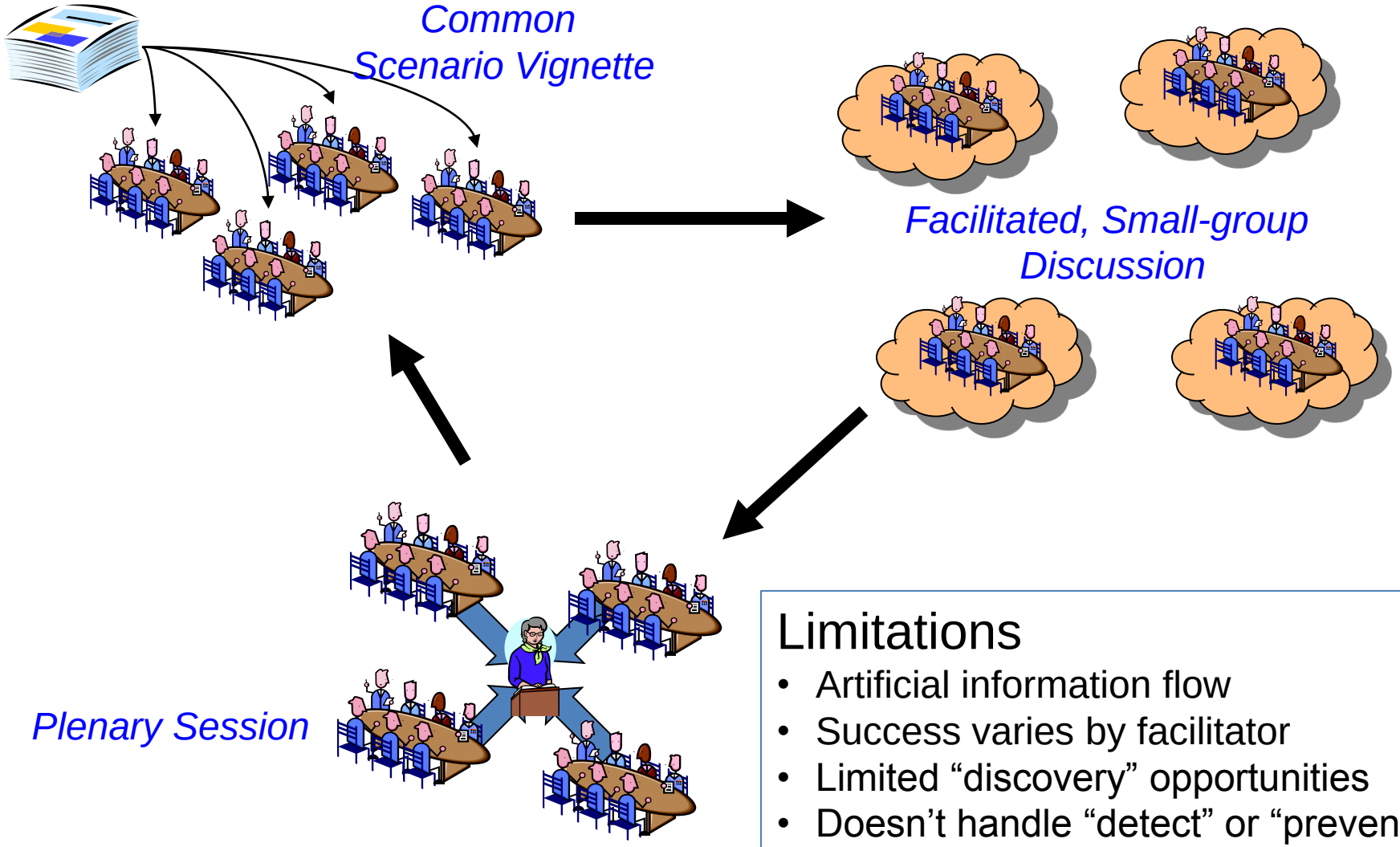
- Defined formats, documentation, and processes
- Correctly focused on improvement planning
- Rich history of success in *physical* domains
- Fairly robust formal program

… so why talk about it?

Seminar
Workshop
TTX
Game

Drill
Functional Exercise
Full-Scale Exercise

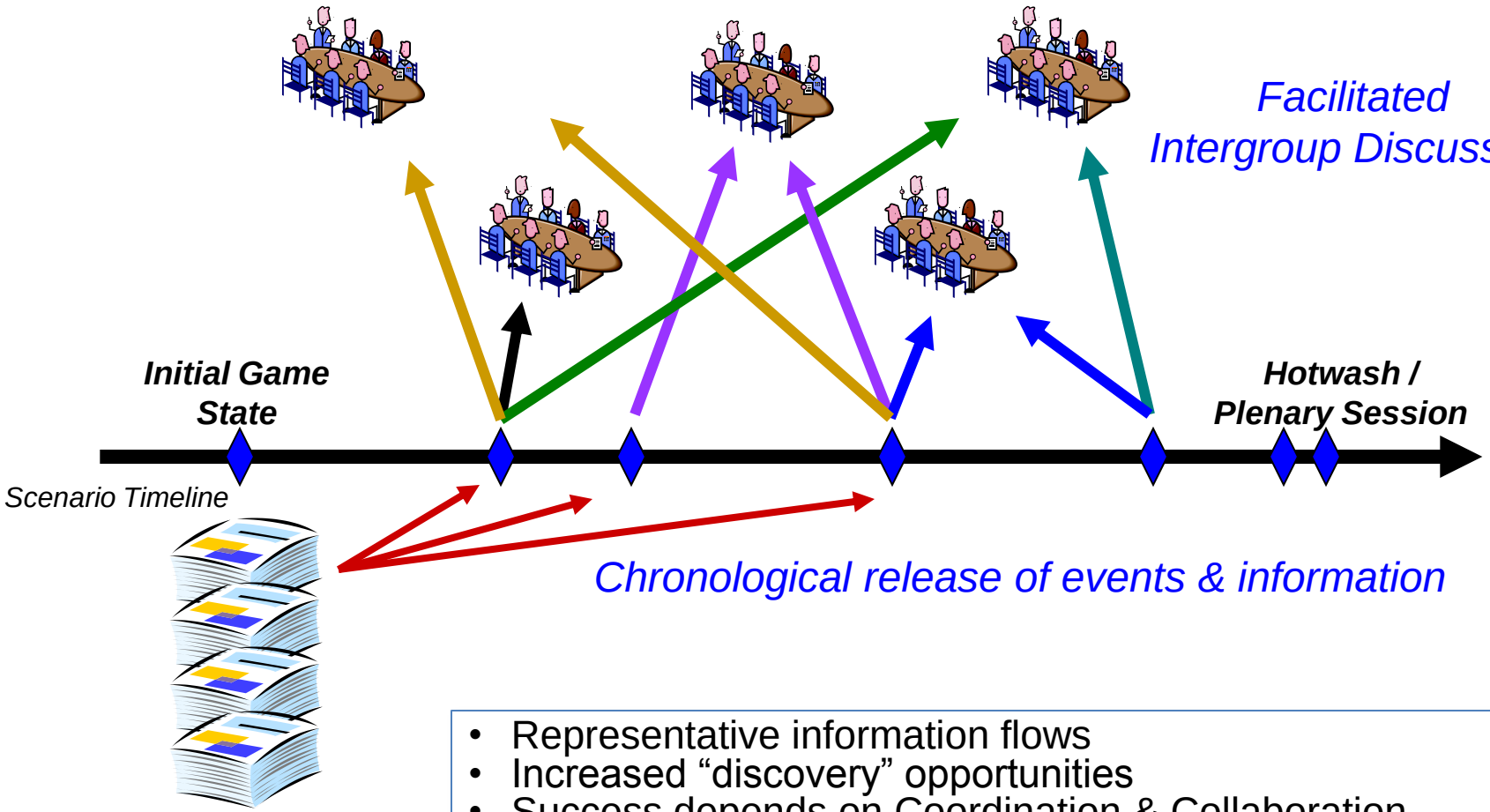
Typical Tabletop (cyber) Exercise



Limitations

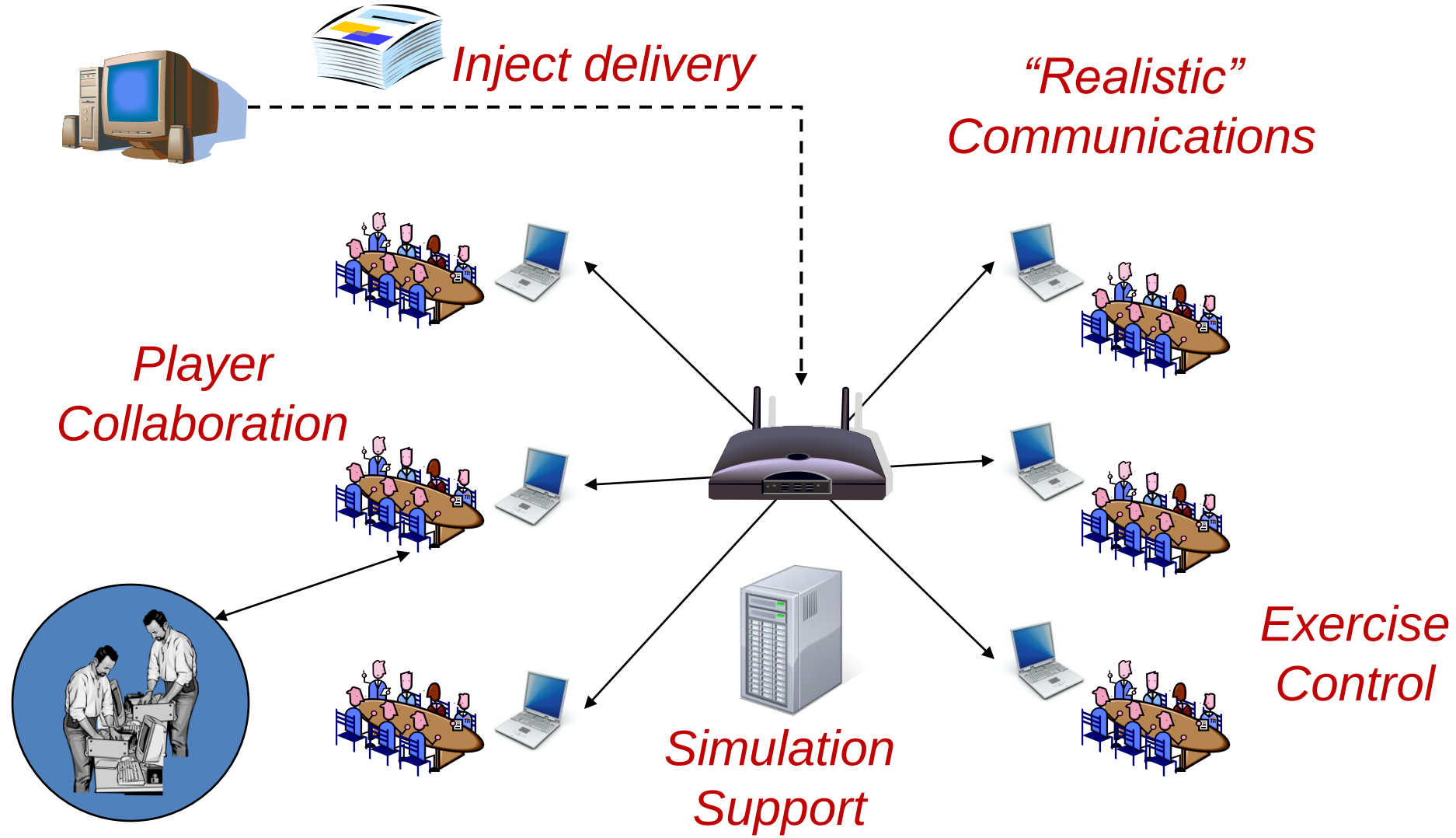
- Artificial information flow
- Success varies by facilitator
- Limited “discovery” opportunities
- Doesn’t handle “detect” or “prevent” activities (= cyber)

Advanced Tabletop Format



- Representative information flows
- Increased "discovery" opportunities
- Success depends on Coordination & Collaboration
- Allows disparate training audience (e.g. Operations & IT staff)

System Extensions / Options

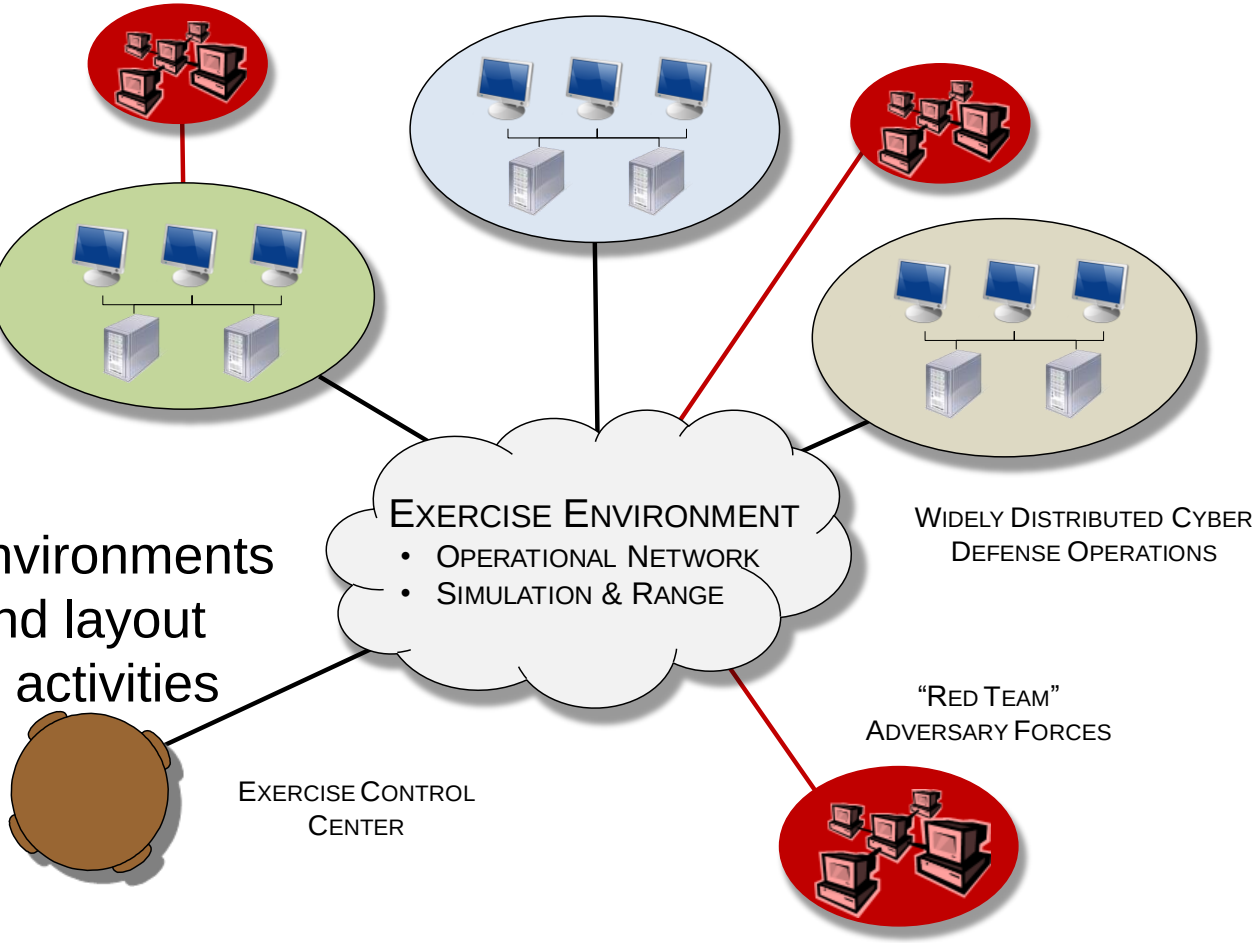


What is an "Advanced Cyber Exercise"…?

- Relevant models
  - HSEEP-defined *Full-Scale Event*
  - *BLACK DEMON*

Attributes

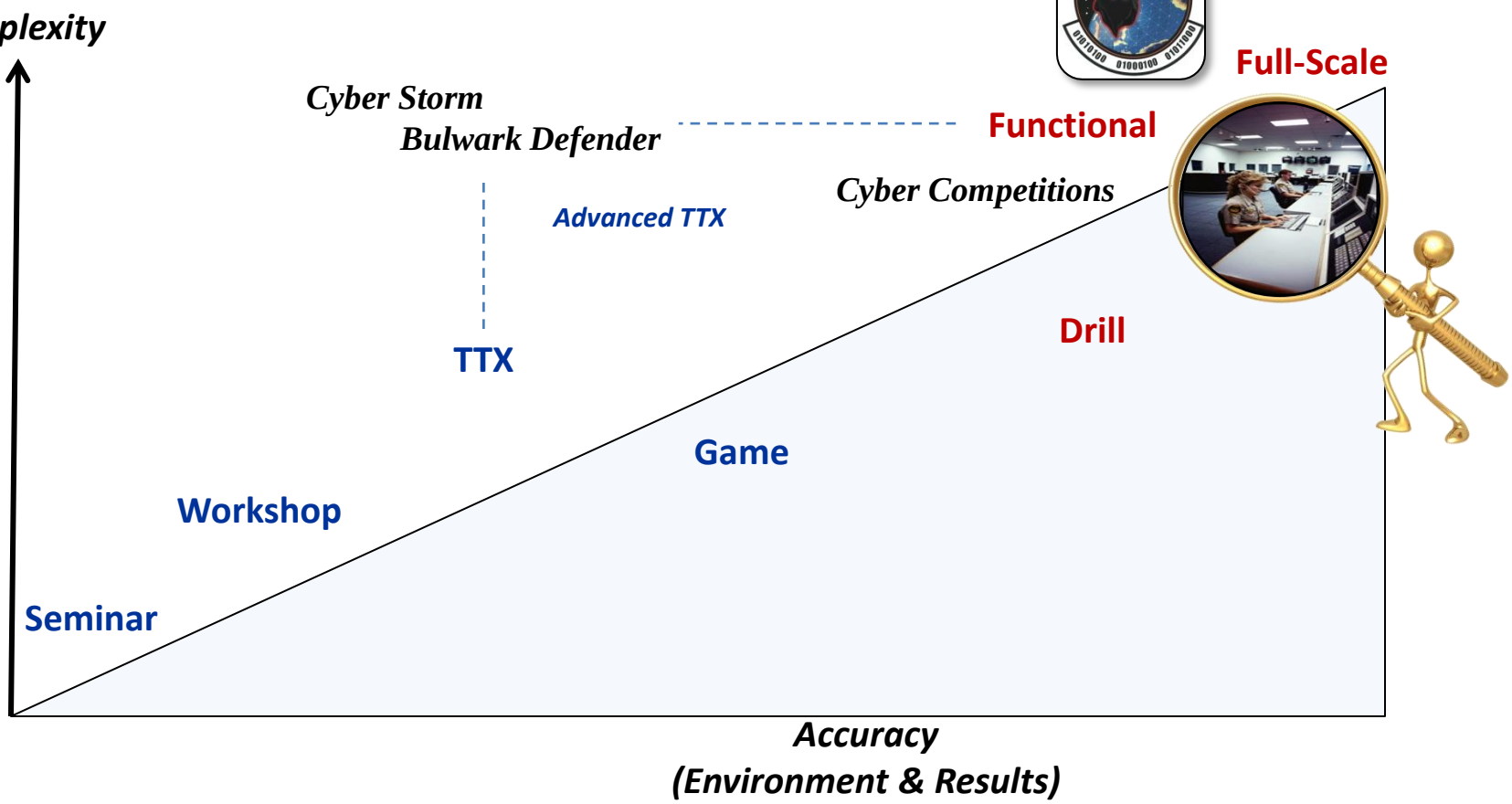
- Hands-on, technical
- Threat emulation
- Realistic operating environments
  - Same systems and layout
- Spans cyber defense activities



Current State of Play

Assessment:

- Private Sector gaining experience in formal exercise processes
- *Necessity* and *Invention* beginning to intersect
- …but, State of the Art not where it could be; need to "raise the bar"



…how do we raise the bar?

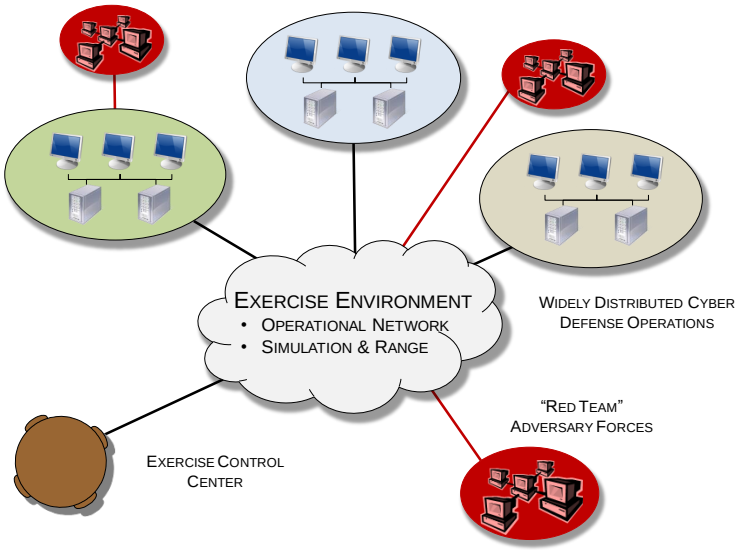
METHODS & PRACTICES

THE "ART" OF EXERCISES

Raising the Bar

… means identifying and developing methods and practices that will:

- Increase Realism
- Manage Complexity
- Foster Repeatability



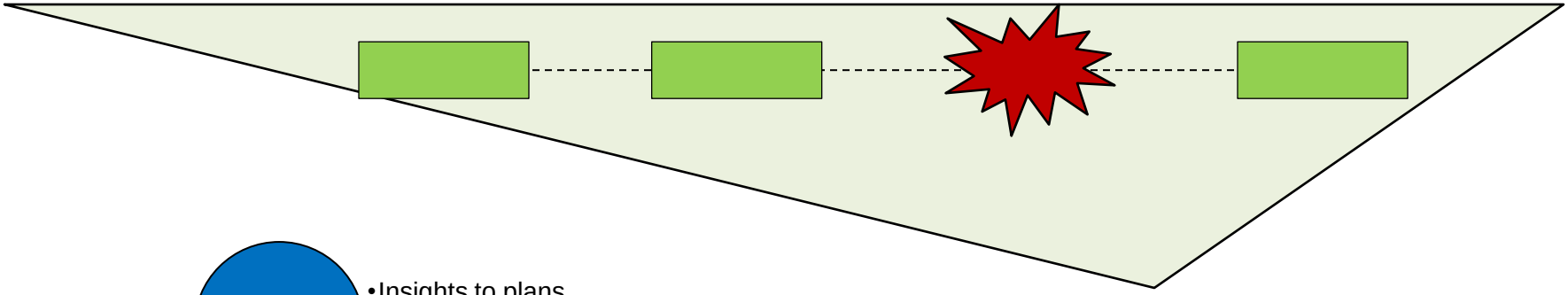
Innovation in:

- Scenario planning
- Operational networks and live-action aggressors
- Simulators and Ranges

… the time in an exercise when the MOST learning takes place

SCENARIO DEVELOPMENT & PLANNING

Scenario Planning Team



Trusted Agent
- Insights to plans, expected responses, systems accesses

"Here's how they'll respond…"

Exercise Control
- Develops injects and control requirements

"Here's how we'll control …"

Evaluation
- Develops assessment criteria and understands expected responses

"Here's what we'll look for…"

Threat
- Develops threat activities, capabilities, and "Red Campaign"

"Here's what we'll do …"

Scenario Planning

"What kind of scenario should we have?"

Effect

"I want to disrupt public access to my online services"

Threat

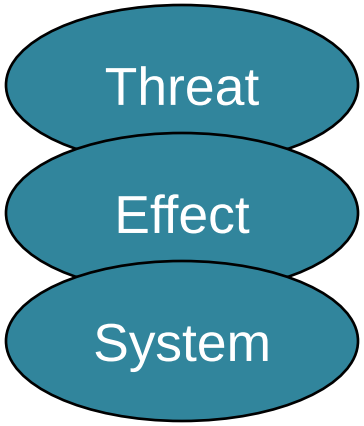
"I want to see a botnet attack scenario"

System

"I want an attack against the vehicle registration system"

… you must be ready to accommodate all three perspectives.

Scenario Planning



Consider

- Your incidents (“*First-hand Knowledge*”)
- Publicly reported activities (“*Researched*”)
- Creatively developed events (“*What If…*”)

- Critical information assets
- Risk assessments
- Known deficiencies
- Demonstrated capabilities
- *What keeps you up at night?*

Determine Operational Concerns

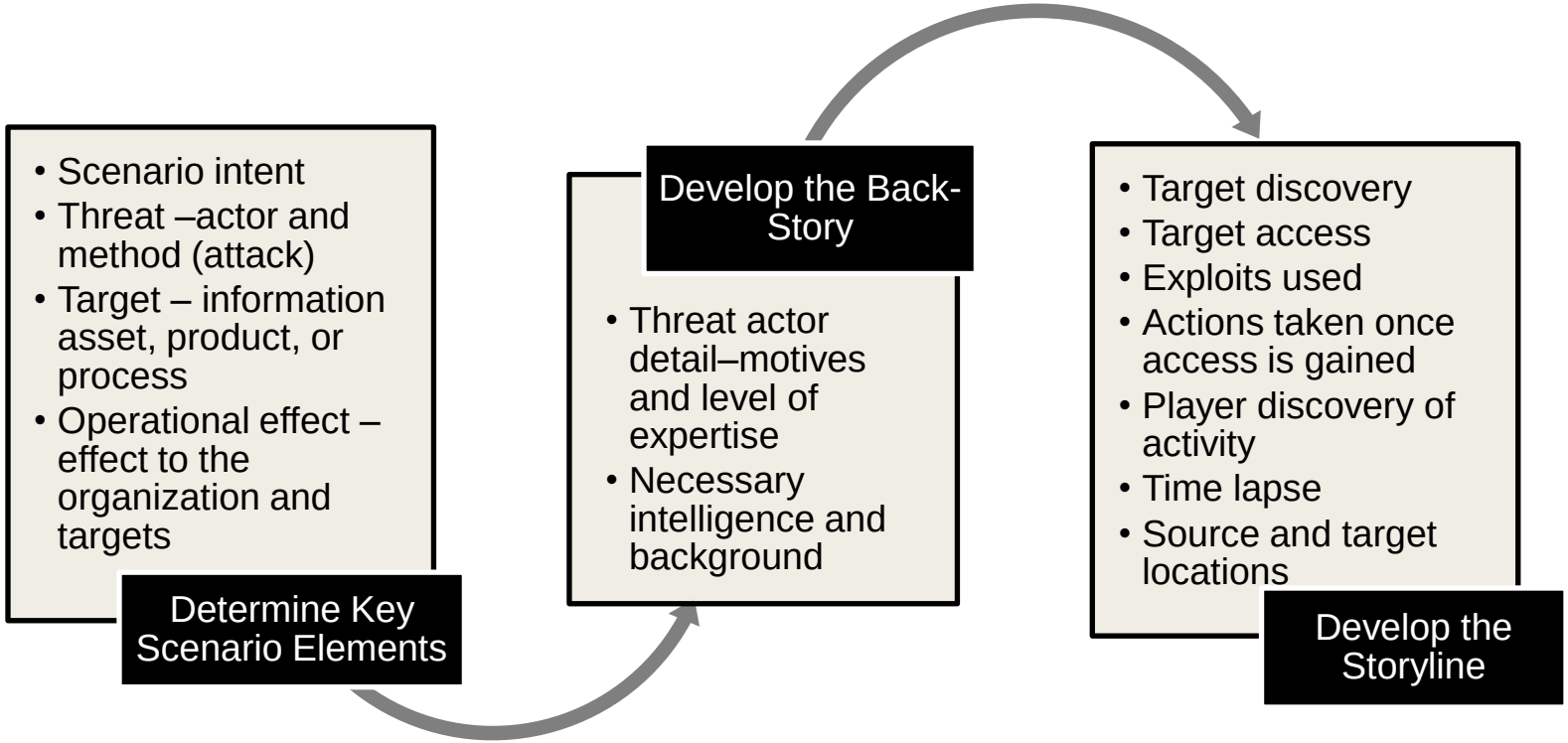
Determine Critical Capabilities

- Organizational capabilities, activities, or tasks
- Target Capabilities List (TCL), Universal Task List (UTL)

- Activities to test, evaluate, or train
- Simple, measurable, attainable, realistic, and task-oriented

Determine Exercise Objectives

Scenario Planning (cont.)



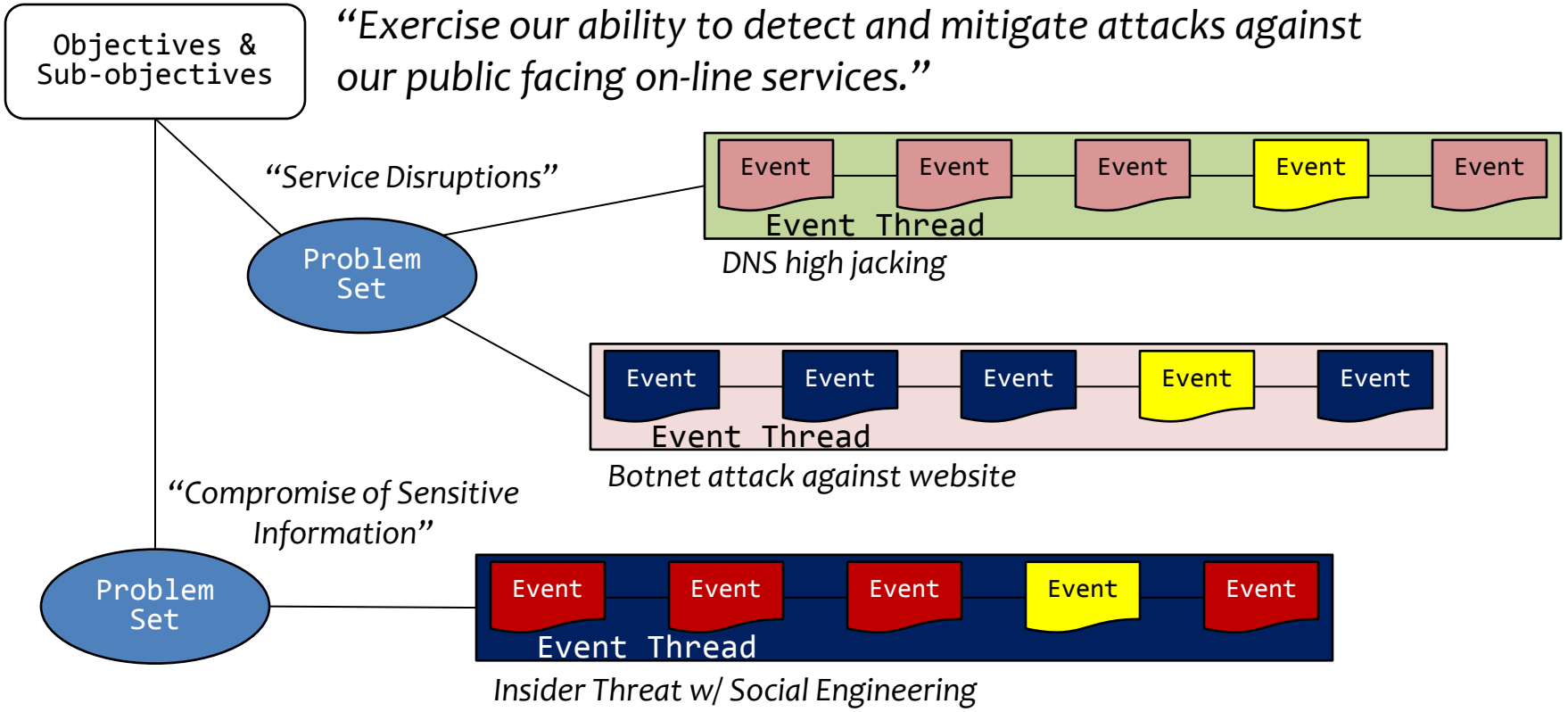
Key Scenario Elements affect:

… who you get to participate

… what expertise you need for planning

… what procedures you focus on for execution

Organizing the Events



How does this look in a MSEL?

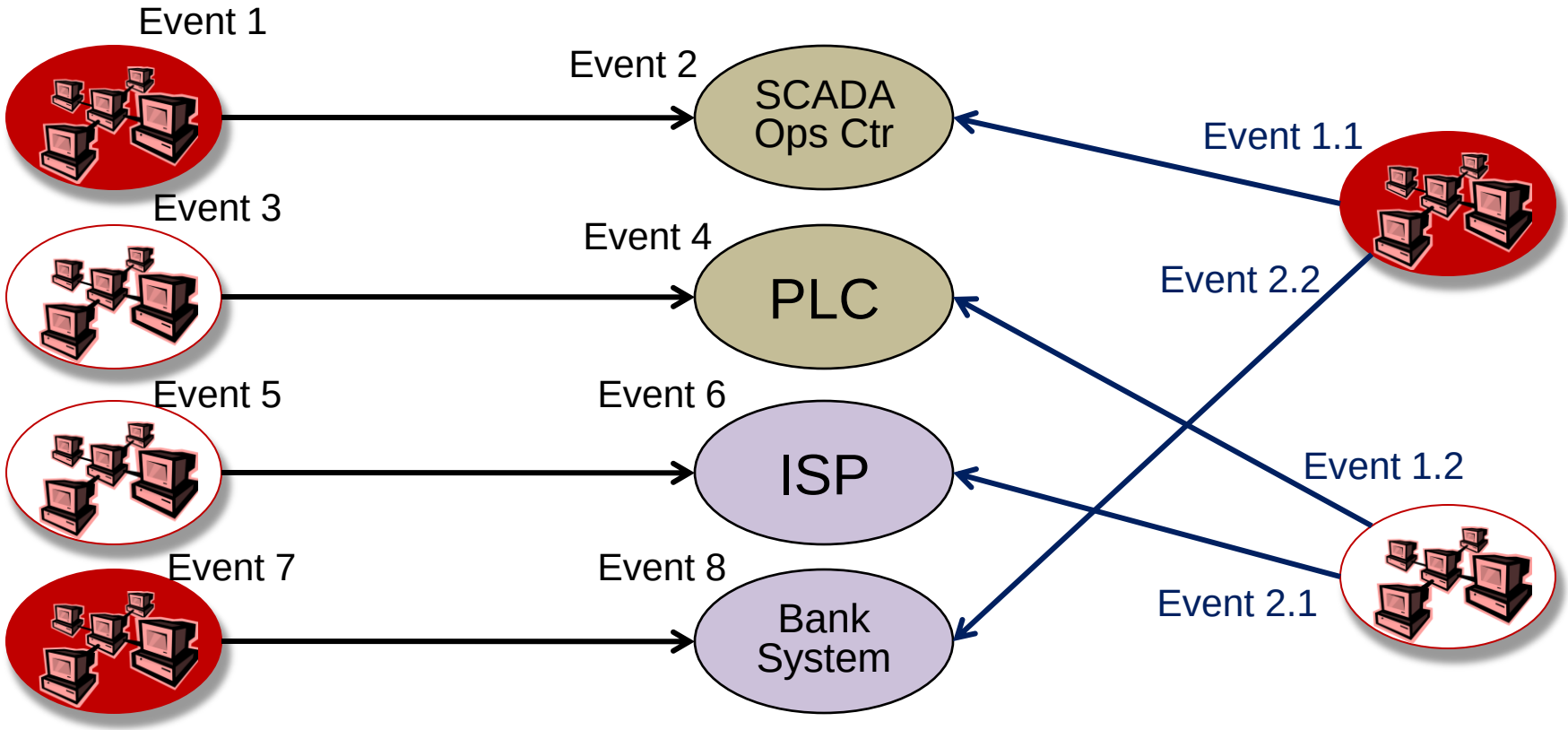
Managing the Complexity

For a TTX … this might be sufficient

"Cyber terrorists conducted a large-scale cyber attack that shut down portions of the electric grid and disrupted on-line banking transactions."

Traditional MSEL …

"Enhanced" MSEL …



Enhanced MSEL

HSEEP MSEL

- designated scenario time
- event synopsis
- name of the controller responsible for delivering the inject
- special delivery instructions
- task and objective to be demonstrated
- expected action, intended player, notes

Enhancements

- Problem Set
- Event Thread
- **Estimated event end time (duration)**
- Environment configuration actions
- Event instructions
  - Controller instructions
  - Evaluator cues / instructions
  - Aggressor actions / instructions

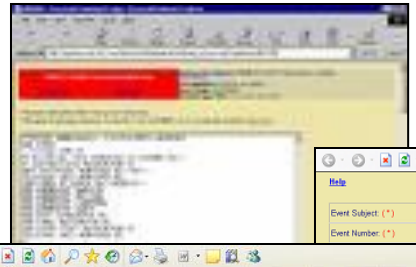
Playbooks tailored to location, function, or event thread

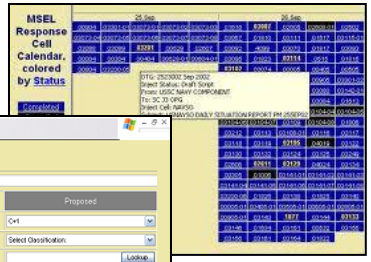
Scenario Planning Tools … briefly

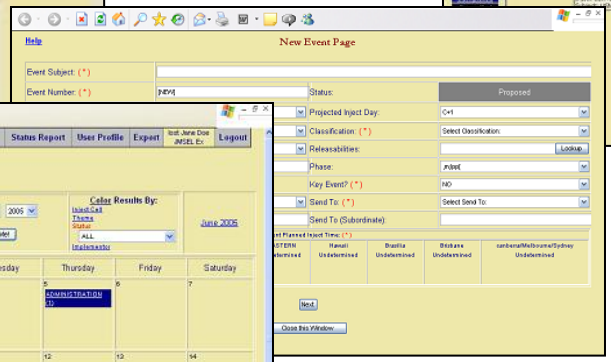
Microsoft® Office, Visio, Project

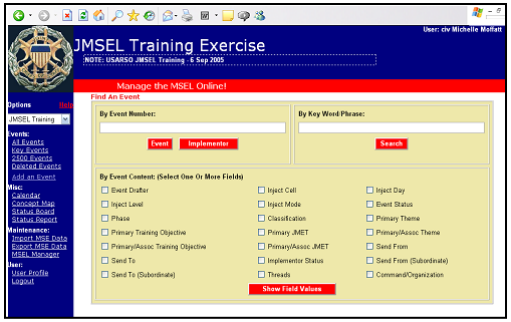
1st Generation

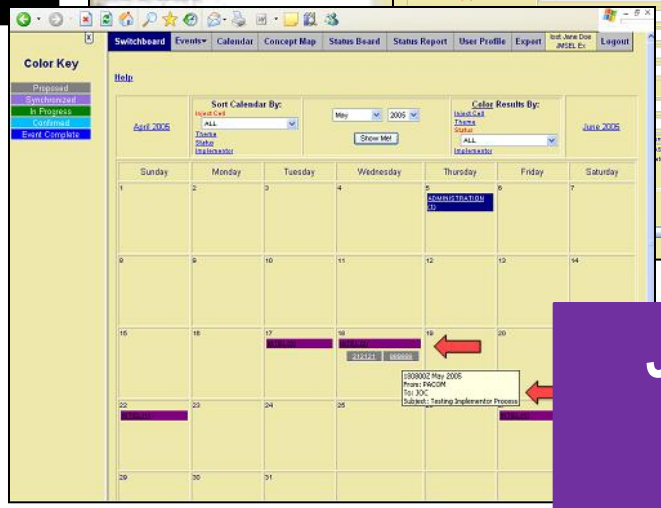
National Exercise Master Scenario Events List (NxMSEL)









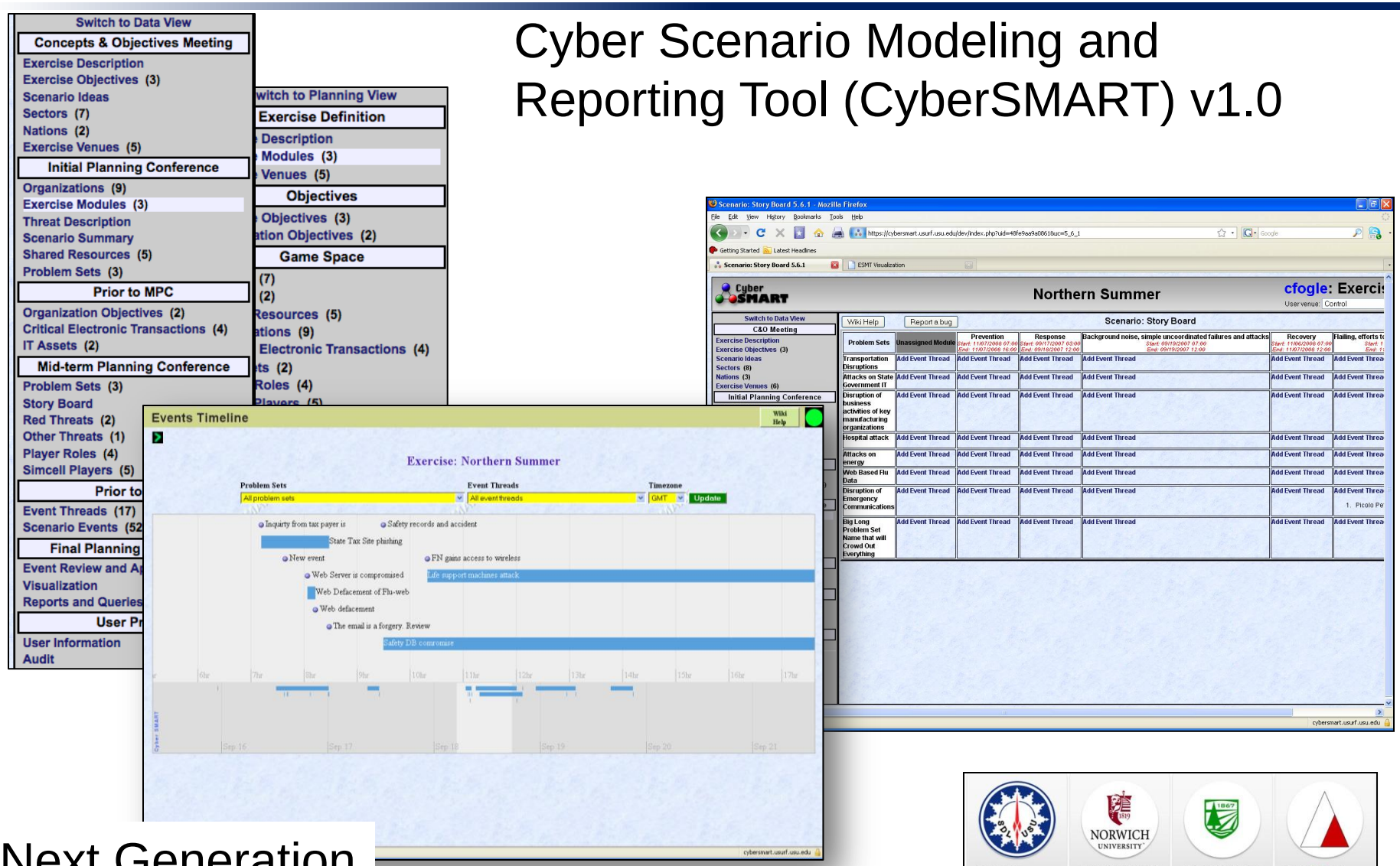


2nd Generation

Joint Master Scenario Events List (JMSEL)

Scenario Planning Tools … briefly

Cyber Scenario Modeling and Reporting Tool (CyberSMART) v1.0



Next Generation

Utah State University Research Foundation

Norwich University Applied Research Institutes

Dartmouth College Institute of Security Technology Studies

Delta Risk, LLC

… after the planning, EXECUTE

LIVE-ACTION AGGRESSORS & PLAYING ON THE OPERATIONAL NETWORK

Live-action aggressors … What's in a name?

Vulnerability Assessment Team

"Dig around, see what you can find, and document the problem – maybe a recommended fix-action, too"

Red Team

"Dig around, see what you can find, and clearly demonstrate or document the impact"

Aggressor

"Be the specific adversary – read up on their TTP, get their tools or techniques, and execute a structured battle plan while providing *requested* stimulus"

"THREAT EMULATION"

… and don't forget skill and maturity

Exercising on Operational Networks

10 missions; only 2 on operational network
… but it changed with demonstrated capability

- ✓ "Low and Slow" probing, scanning, and enumeration
- ✓ Denial of Service (systems)
- ✓ Rogue systems & access points
- ✓ Phishing – email and web
- ✓ Zero-day
- ✓ Host compromise (virus/malware, hacked)
- ✓ Data exfiltration
- ✗ Worm attack
- ✗ Denial of Service (bandwidth)
- ✗ Widespread Botnet attack (target or zombie)

Considerations for Exercising on Ops Networks

- IP / host deconfliction tables; map aggressor exercise IP space to “real-world”
- Use known vulnerabilities; unpatch or misconfigure the system for execution
  - Block external access at the firewall; restrict by IP address
- Use tools to monitor traffic to exercise systems
- Leave system disconnected from the network until needed within the exercise
- Set an administrator password; use an access authentication and traffic encryption
- Use Media Access Control (MAC) address filtering and limit Dynamic Host Configuration Protocol (DHCP) lease

… for those things you just can't do on the network

SIMULATORS AND RANGES

Simulators and ranges

- BLACK DEMON ranges
  - Fielded net defense tools, separate network that looked like Air Force NOSCs and NCCs; Simple traffic generation, not stateful
- Simulator Training Exercise (SIMTEX)
  - Formal program that evolved from BLACK DEMON; fixed-architecture duplicated AF net defense apparatus
  - Rapid improvements in traffic generation and realistic attack signatures
  - Used in BLACK DEMONs and BULWARK DEFENDER

Simulators and ranges

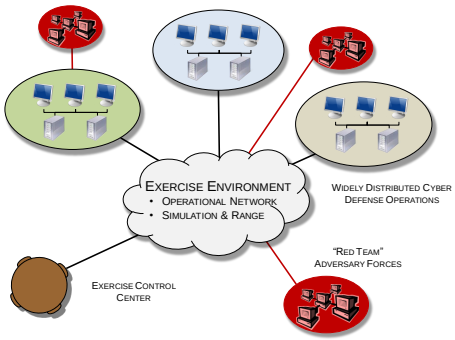
- Exercise Network (XNET)
  - Developed by Software Engineering Institute at Carnegie Mellon University
  - Virtual machine technology and “push-button” deployment of multiple, simultaneous exercise environments; customized scenarios
  - Centralized, isolated, and dedicated exercise environment significantly reduces setup and configuration time
  - Easily customized Threat scenarios and realistic threat model
    - Timeline and Event Library, Drag and Drop attacks/anomalies
  - Automated data collection
    - Real-time readiness metrics
  - Allows for experienced cadre to enable local crew training

Simulators and ranges

- Cyberoperations Enhanced Network & Training Simulators (CENTS™)
  - Developed by EADS North America, Defense Security and Systems Solutions, Inc. (DS3)
  - Emulates a desired operational network architecture & uses existing Wide Area Network transport
  - Virtual Machine Technology
    - Network sensor systems, switches, routers, firewalls, servers, domain controllers, email, and other various network services normally found in most computer network architectures
  - Vulnerabilities can be built in to the simulator to provide the crew exposure
  - Operated both as a single system or a network of systems connected by a secure Virtual Private Network (VPN)
    - Cybersecurity Network Training Simulator (CYNTRS®) for crew training
    - Hands-On-Training Simulator (HOTSIM®) for classroom training

Final Thoughts on Raising the Bar…

- Community dialogue on advanced cyber exercise methods and practices
  - Simulator and range technologies
  - Planning methodologies and tools
  - Cyber exercises and HSEEP



- Courses for cyber exercise planning and execution
  - Indoctrination for all-hazards practitioners
  - Threat emulation and skills training, certification
- Scenario templates
  - Lessons learned, central repository of best practices

Contact

- Chris Fogle, CISSP
  Delta Risk, LLC
  cfogle@delta-risk.net

- ***Strategic Consulting & Policy Development***
- ***Operational Concept Development***
- ***Security Program Assessment***
- ***Advising technology development***
- ***Cyber Exercises - Planning & Execution***
- ***Training Programs & Courseware***
- ***Expert Witness Services***